



## FEDERAL COMMUNICATIONS COMMISSION

### 47 CFR Part 64

[CG Docket No. 12-129; PS Docket No. 21-343; FCC 21-108; FRS 53657]

Enhancing Security of Public Safety Answering Point Communications

**AGENCY:** Federal Communications Commission.

**ACTION:** Proposed rule.

**SUMMARY:** In this document, the Commission seeks to gather updated information and propose how best to fulfill Congress' goal of protecting Public Safety Answering Points (PSAPs) from disruptive robocalls in a manner that avoids the potential security risks of making registered PSAP numbers available to those claiming to be autodialer operators. Specifically, the Commission proposes that voice service providers be required to block autodialed calls made to PSAP telephone numbers on the PSAP Do-Not-Call registry. The Commission takes this action to satisfy its statutory obligations under the Middle Class Tax Relief and Job Creation Act of 2012 (Tax Relief Act).

**DATES:** Comments are due on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER], and reply comments are due on or before [INSERT DATE 45 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

**ADDRESSES:** You may submit comments, identified by CG Docket No. 12-129 and PS Docket No. 21-343, by any of the following methods:

- *Electronic Filers:* Comments may be filed electronically using the Internet by accessing the ECFS: <http://apps.fcc.gov/ecfs/>.
- *Paper Filers:* Parties who choose to file by paper must file an original and one copy of each filing. If more than one docket or rulemaking number appears in the caption of this proceeding, filers must submit two additional copies for each additional docket or

rulemaking number.

Filings can be sent by commercial overnight courier or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.

- Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701.
- U.S. Postal Service first-class, Express, and Priority mail must be addressed to 45 L Street NE, Washington, D.C. 20554.
- Effective March 19, 2020, and until further notice, the Commission no longer accepts any hand or messenger delivered filings. This is a temporary measure taken to help protect the health and safety of individuals, and to mitigate the transmission of COVID-19. See *FCC Announces Closure of FCC Headquarters Open Window and Change in Hand-Delivery Policy*, Public Notice, DA 20-304 (March 19, 2020), <https://www.fcc.gov/document/fcc-closes-headquarters-open-window-and-changes-hand-delivery-policy>.

**FOR FURTHER INFORMATION CONTACT:** Richard D. Smith of the Consumer and Governmental Affairs Bureau at (717) 338-2797 or [Richard.Smith@fcc.gov](mailto:Richard.Smith@fcc.gov).

**SUPPLEMENTARY INFORMATION:** This is a summary of the Commission's Further Notice of Proposed Rulemaking (*FNPRM*), in CG Docket No. 12-129 and PS Docket No. 21-343, FCC 21-108, adopted on September 30, 2021 and released on October 1, 2021. The full text of the document is available for public inspection and copying via the Commission's Electronic Comment Filing System (ECFS). To request materials in accessible formats for people with disabilities (Braille, large print, electronic files, audio format), send an e-mail to [fcc504@fcc.gov](mailto:fcc504@fcc.gov) or call the Consumer and Governmental Affairs Bureau at 202-418-0530 (voice).

This matter shall be treated as a “permit-but-disclose” proceeding in accordance with the Commission’s *ex parte* rules. 47 CFR 1.1200 through 1.1216. Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentations must contain summaries of the substances of the presentations and not merely a listing of the subjects discussed. More than a one or two sentence description of the views and arguments presented is generally required. *See* 47 CFR 1.1206(b). Other rules pertaining to oral and written *ex parte* presentations in permit-but-disclose proceedings are set forth in § 1.1206(b) of the Commission's rules, 47 CFR 1.1206(b).

## **INITIAL PAPERWORK REDUCTION ACT OF 1995 ANALYSIS**

The *FNPRM* seeks comment on proposed rule amendments that may result in modified information collection requirements. If the Commission adopts any modified information collection requirements, the Commission will publish a notice in the **Federal Register** inviting the public to comment on the requirements, as required by the Paperwork Reduction Act. Pub. L. 104-13; 44 U.S.C. 3501-3520. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, the Commission seeks comment on how it might further reduce the information collection burden for small business concerns with fewer than 25 employees. Pub. L. 107-198; 44 U.S.C. 3506(c)(4).

## **SYNOPSIS**

### **A. Extent of the Problem**

1. In this *FNPRM*, the Commission seeks updated information since the PSAP Do-Not-Call registry was adopted in 2012 about the magnitude of the problem that the PSAP Do-Not-Call registry is intended to address—i.e., the frequency of autodialer-initiated calls to PSAPs’ telephone lines and the extent of the disruption and other harms that these calls cause. *See Implementation of the Middle Class Tax Relief and Job Creation Act of 2012, Establishment of a Public Safety Answering Point Do-Not-Call Registry*, CG Docket No. 12-129, Report and Order, 27 FCC Rcd 13615 (2012). In adopting the registry rules, the Commission noted that autodialers

can tie up public safety lines, divert critical responder resources from emergency services, and impede the public's access to emergency lines.

2. The Commission seeks comment on the extent to which autodialed calls continue to be a problem for PSAPs. Has the number of such unwanted calls changed in any significant way since 2012? For example, have technological changes resulted in more unwanted autodialed calls being made to PSAPs or have any new technological or regulatory solutions, such as blocking technologies, arisen that allow PSAPs to better protect themselves from unwanted calls? Does the extent of this problem vary depending on whether the autodialed calls are voice calls or texts? Are there situations in which entities that intended to disrupt PSAP operations used autodialers or similar technologies in denial-of-service attacks to disrupt the provision of emergency services? How do those incidents shed light on the risk and potential harms that might result from the misuse of registered PSAP numbers? Have such incidents increased since 2012, as technology has changed? Are there new or evolving robocall threats to PSAPs that the registry is not designed for or otherwise cannot address? If so, are there ways to adapt the registry to such threats?

3. To what extent does the recent Supreme Court decision addressing the Telephone Consumer Protection Act's (TCPA's) definition of "automatic telephone dialing system" impact the efficacy of the PSAP Do-Not-Call registry? *See Facebook, Inc. v. Duguid*, 141 S.Ct. 1163, 1168-73 (2021). For example, does the Supreme Court's decision potentially narrow the types of equipment that fall within that definition, and thus limit the number of callers subject to the prohibition on autodialing registered PSAP numbers? If fewer callers are deemed "autodialers" under the ruling than previously, does that have implications for the Commission's assessment of the security risk by potentially reducing the number of callers that will need to access the registry? Correspondingly, does it change the protections afforded to PSAPs by narrowing the types of callers that are prohibited from calling registered telephone numbers?

## **B. Call Blocking Proposal**

4. In light of potential security concerns involved with granting access to the registered PSAP numbers to a broad range of autodialer operators as the means to facilitate compliance with the PSAP Do-Not-Call registry as contemplated in 2012, the Commission proposes that voice service providers block autodialed calls made to registered PSAP telephone numbers on the PSAP Do-Not-Call registry. As the means to identify the calls to be blocked, the Commission's rules already require autodialer operators seeking access to the registry to provide certain information including "all outbound telephone numbers used to place autodialed calls, including both actual originating numbers and numbers that are displayed on caller identification services." *See* 47 CFR 64.1202(d). The Commission proposes that such registered "outbound" telephone numbers used to make autodialed calls be provided to voice service providers as the means to identify those autodialed calls that should be blocked when made to registered PSAP numbers.

5. The Commission proposes to give voice service providers access to the PSAP telephone numbers and outbound autodialer telephone numbers registered on the PSAP Do-Not-Call registry. The Commission further proposes to require voice service providers to block any calls that originate from a registered autodialer number when made to a registered PSAP telephone number. Under this approach, access to the registered PSAP telephone numbers is restricted to more easily verified voice service providers that can ensure compliance by blocking calls made to the PSAP telephone numbers rather than entrusting compliance to an unknown number of robocallers whose identity and intentions in seeking access to the database may be difficult to confirm. Specifically, the Commission seeks comment on whether such an approach would alleviate the security risks associated with allowing access to a centralized database of PSAP numbers to all autodialer users who register. Does granting voice service providers access to registered PSAP telephone numbers create any new security issues? If so, how should the Commission minimize those concerns? How can the Commission ensure the security of the PSAP Do-Not-Call registry database from malicious actors?

6. *Responsible Voice Service Providers.* The Commission seeks comment on which voice service providers should be subject to the blocking requirement. Should one voice service provider in the call path be responsible for blocking calls from registered autodialer telephone numbers to registered PSAP telephone numbers? Are certain voice service providers, such as those originating or terminating calls or those voice service providers that are also covered 911 service providers, better suited to carry out this obligation?

7. *Emergency Autodialed Calls.* The Commission seeks comment on whether to limit its blocking requirement only to non-emergency autodialed calls. The current rules prohibit operators of robocalling equipment from using such equipment to contact registered PSAP numbers “other than for an emergency purpose.” See 47 CFR 64.1202(c). Should the Commission retain this distinction or instruct voice service providers to block any calls from a registered autodialer number to a registered PSAP number? Are there situations when autodialer users may use autodialing equipment to make an emergency call? If so, how should the Commission account for such a possibility? Should the Commission grant access to the registry only to those autodialer numbers that are used solely for non-emergency purposes? Should the Commission adopt rules that establish a presumption that all calls from registered autodialer telephone numbers are non-emergency calls, and if so, what steps should the Commission take to ensure emergency calls to PSAPs are not inadvertently blocked? Are there any other barriers, costs, or considerations that should be taken into account in adopting rules that require voice service providers to block non-emergency calls from registered autodialer telephone numbers to registered PSAP numbers?

8. *Preventing Unauthorized Disclosure of Registered Numbers.* The Commission proposes and seeks comment on extending the existing restrictions on disclosure and dissemination of registered numbers to voice service providers that might be granted access to the registry under our proposed approach. See 47 CFR 64.1202(f); 47 U.S.C. 1473(c)(1). Are the current restrictions sufficient or should the Commission adopt new or different restrictions to prevent the

unauthorized disclosure of registered numbers?

9. *Erroneous Blocking.* Is requiring the blocking of autodialed calls technically feasible for voice service providers? If so, can those programs ensure that calls PSAPs wish to receive are not blocked? Should the Commission consider a safe harbor from liability for good faith blocking of phone calls to PSAPs from originating numbers that are erroneously entered into the registry? Should autodialer operators be afforded a safe harbor from liability when they have submitted an outbound telephone number to the PSAP Do-Not-Call registry, but the call is not blocked through the fault of the voice service provider or registry administrator?

10. *Verifying and Updating the Registry.* Are there other safeguards the Commission should adopt to ensure that emergency phone calls are not affected by the call blocking proposal to avoid inadvertently blocking legitimate emergency calls? The current rules require that all contact information provided by an autodialer operator to gain access to the registry, including the outbound telephone numbers used to place autodialed calls, be updated within 30 days of any change to this information. *See* 47 CFR 64.1202(d). Is this requirement sufficient to ensure that the database of telephone numbers used to identify those autodialed calls to be blocked remains updated to remove telephone numbers that are no longer used to make autodialed calls and add new telephone numbers that are used to make autodialed calls? Or should the Commission consider any new or different requirements to ensure that the database of registered telephone numbers used to make autodialed calls remains accurate over time? Are there alternative methods and sources that should be employed by the voice service provider or registry administrator to ensure that only non-emergency calls are blocked to registered PSAP telephone numbers? Is there a cost-effective means for voice service providers to track the use of such telephone numbers to determine if they have been recently ported to non-autodialer users? Should voice service providers be required to report to the Commission the number of blocked autodialer calls to PSAPs in order to help the Commission assess how frequently such calls occur and whether the registry is effective?

11. *Security Risks.* Would a call blocking requirement raise the risk that a malicious actor could reverse-engineer a list of PSAP numbers by determining what calls have been blocked? Would that create any additional security risk for PSAPs? If there is such a risk, would this allow bad-actor callers to spoof the PSAP number and avoid all blocking under our existing rule limiting blocking emergency calls from PSAPs? If so, what could the Commission do to address this concern? Should the Commission's transparency and redress requirements for blocked calls apply to blocking done pursuant to a PSAP Do-Not-Call registry? *See* 47 CFR 64.1200(k)(8). Are there other factual, legal, or policy factors that the Commission should consider before allowing voice service providers to block calls to PSAP numbers that are used for emergency purposes? Alternatively, would such a requirement raise the risk that a malicious actor may purposely register non-autodialing outgoing numbers into the registry in order to prevent legitimate emergency callers from contacting PSAPs? If so, how can the Commission address such a concern? Are there any other potential security concerns the Commission may need to address?

12. *Costs and Impact on Small Business.* The Commission seeks comment on the impact of its proposal on small businesses and any potential alternatives that may reduce the impact of autodialed calls on PSAPs without imposing burdens on such small businesses. The Commission tentatively concludes that the benefits associated with its proposal exceed the costs and seeks comment on this tentative conclusion. The Commission seeks comment on any specific cost concerns associated with its proposal. Are there ways to mitigate any costs or burdens on smaller voice providers associated with implementing a call blocking approach to satisfy the statutory obligation to create a PSAP Do-Not-Call registry?

13. *Statutory Authority.* The Commission believes that the proposed approach satisfies its statutory obligation to "create a specialized Do-Not-Call registry" for PSAPs. *See* 47 U.S.C. 1473. In addition, the Commission believes that this approach satisfies its statutory requirement to "provide a process for granting and tracking access to the registry by the operators of



automatic dialing equipment.” *See* 47 U.S.C. 1473(b)(3). The Commission seeks comment on this analysis of the statutory requirements contained in section 6507(b) as applied to the call blocking proposal in the *FNPRM*, including the extent to which the Commission’s current rules must be amended to implement this proposal.

### **C. Do-Not-Call Registry 2012 Security Concerns**

14. The Commission seeks comment on its assessment of the seriousness of the security risks associated with housing registered PSAP telephone numbers in a centralized database and granting access to those numbers to callers purporting to need them to comply with the rules as contemplated in 2012. The Commission is particularly interested in comments from PSAPs, law enforcement agencies, and national security agencies on these risks. To what extent, if any, would granting access to a list of PSAP numbers enhance the ability of bad actors to initiate a denial-of-service attack on a PSAP? Are there other comprehensive sources of PSAP telephone numbers already available, such that incremental risks added by the registry would be minimal? Even if some individual PSAP numbers are obtainable from alternative sources, to what extent would access to a single centralized database of such numbers increase the security risks of misuse of such numbers? On balance, do these security concerns outweigh the potential protections a registry affords from unwanted autodialed calls? How might the Commission best address the security concerns posed by a centralized database of PSAP telephone numbers that would allow the Commission to move forward with the creation of a PSAP Do-Not-Call registry, as contemplated in 2012, in a manner that does not jeopardize PSAPs and emergency callers that rely on PSAPs?

15. To what extent do the significant potential monetary penalties for PSAP Do-Not-Call violations and for unauthorized dissemination or distribution of the registered PSAP numbers impact the Commission’s analysis of the risks of potential abuse? To what extent is the effectiveness of such monetary penalties undermined when dealing with individuals or entities who seek to intentionally disrupt the provision of emergency services and make efforts to

conceal their identity, or who are foreign actors against whom it may be difficult or impossible to enforce such penalties? Does the implementation of STIR/SHAKEN caller ID authentication technology, or the efforts of the registered traceback consortium to trace calls back to their source, make it less likely that callers initiate denial-of-service attacks on PSAPs by making it easier to determine the source of a call?

#### **D. Alternative Solutions to the Do-Not-Call Registry Security Issues**

16. *Enhanced Caller Vetting.* If the call blocking proposal to protect PSAPs from unwanted autodialed calls proves unworkable, are there other mechanisms or safeguards that the Commission could implement to effectively vet the identity of users who seek access to registered PSAP numbers to reduce the likelihood of providing access to those telephone numbers to bad actors that might misuse these numbers, and if so, what are they? The Commission's rules already require that entities seeking access to the registry provide certain contact information including, for example, the names under which the registrant operates, a business address, a telephone number, an email address, and a contact person. *See* 47 CFR 64.1202(d). Is this information sufficient to confirm the identity and intent of the party seeking access to the registry or should the Commission impose additional or different requirements? How could the Commission prevent parties that seek access to the registry for malicious purposes from submitting false information to circumvent its review and gain access to the registry under false pretenses? Would any such measures be consistent with section 6507(b)(3), which directs the Commission to "provide a process for granting and tracking access to the registry by the operators of automatic dialing equipment?" For instance, does the Commission have discretion under that provision to limit access only to certain operators? Is such discretion in that regard supported by the fact that section 6507(b)(4) directs the Commission to "protect the list of registered numbers from disclosure or dissemination by parties granted access to the registry?" Is there any level of cost-effective vetting the Commission could do that would sufficiently guard against improper use of the registry? The Commission asks commenters to

provide cost information on any suggested mechanisms or safeguards.

17. *Improved Data Security Requirements.* Even with sufficient vetting of registry users, would there remain significant risks that PSAP telephone numbers could be disseminated, either intentionally or unintentionally, as part of that process (e.g., through carelessness or malicious hacking)? What security measures should the Commission consider to ensure that parties that obtain such sensitive data institute appropriate measures to prevent data breaches? What types of data security requirements might be appropriate? Should any such mechanisms relied upon to protect PSAP telephone numbers from unauthorized access or disclosure be adaptable to address data security issues? If so, would they need to be adaptable in real time or near-real time? How would such adaptation be effectuated as a practical matter?

18. Consistent with section 6507(b)(1), the Commission's rules "permit," but do not require, PSAPs to register "any PSAP telephone numbers associated with the provision of emergency services or communications with other public safety agencies." *See* 47 CFR 64.1202(b). Does the discretion afforded to PSAPs to decide which, if any, of their telephone numbers that they wish to place on the registry allow PSAPs to decide for themselves whether the benefits outweigh the risks of submitting numbers to the registry? How should this impact the Commission's review of the security risks of a PSAP Do-Not-Call registry? Can PSAPs, for example, decide to register only those numbers for which they determine that the protections from unwanted calls outweigh the potential harms from denial-of-service attacks? Do PSAPs have sufficient information to understand the protections and risks afforded by the PSAP Do-Not-Call registry, including an understanding of the types of dialing equipment that would be prohibited from calling those numbers under the TCPA's definition of an "autodialer?" Should the Commission conduct outreach to ensure that PSAPs are aware of the potential benefits and risks of submitting their numbers for inclusion on the registry? Conversely, if PSAPs decline to register their numbers due to the security risk, would that undermine the effectiveness of the PSAP Do-Not-Call registry? What security protections, if any, would be necessary to reassure

PSAPs that the benefits of participating in the registry outweigh the risks? The Commission invites commenters to provide information on the costs and benefits of any proposed security protections.

#### **E. Alternative Technical and Regulatory Solutions**

19. *Other Technological Solutions.* Are there other technological solutions beyond the Commission's call blocking proposal that may have emerged in the near decade since section 6507 became law that the Commission might explore to protect PSAPs from unwanted calls while fulfilling the statute's requirements? For example, could the Commission require callers to filter their autodialed calls through a hardware or software platform that would house an encrypted list of registered PSAP numbers and would be able to block autodialing equipment from making calls to these numbers? Do such technologies exist, and would it be cost effective and technologically feasible to implement such a solution? If such a technological solution does not currently exist, what steps would be needed to develop such technology and what entity or entities might be best suited to do so? What costs would be involved in terms of time and money to develop such a technological fix?

20. How long might it take to identify, develop, and implement any such alternative solution to a PSAP Do-Not-Call registry? What would it cost to create such a solution? Who would maintain the list of telephone numbers housed in such a technological solution, and how often would the technology be updated or would callers be required to install updates? Are there risks that legitimate emergency calls might be blocked if such a system were implemented? Are there other viable alternative technological options that the Commission should consider that satisfy the specific statutory requirements and objectives of section 6507? Alternatively, should the Commission consider certain options—even if they do not satisfy section 6507 in and of themselves—that the Commission could adopt in addition to measures that do satisfy section 6507?

21. Security solutions exist today that can block calls to PSAPs that are determined to be

fraudulent. These solutions become more effective when used in combination with STIR/SHAKEN. Is call blocking at the PSAP a more effective solution? Can PSAPs deploy the same blocking solutions that are used for consumers, or are more specialized solutions required? If blocking is to be based, at least in part, on information produced by STIR/SHAKEN, what information should the terminating provider disseminate to the PSAP to make this determination? If more specialized solutions are required, how do these tools differ from consumer blocking tools? Would the need for PSAPs to deploy this solution place additional technical complexity and/or additional financial burden on PSAPs, and if so, how could this be mitigated? Which type of solutions can be deployed on a wide scale?

22. Apart from provider blocking, do PSAPs themselves have an ability to effectively block unwanted calls? If not, how long would it take and how much would it cost to implement such a blocking solution? Would requiring every autodialed call to identify itself as an automated call using the caller ID information allow PSAPs to block these calls more effectively? Are there any “best practices” that PSAPs might implement to protect themselves from robocalls? For example, the Hospital Robocall Protection Group has issued a report outlining best practices that hospitals can use to protect hospitals against robocalls. Should the Commission consider outlining similar best practices for PSAPs? If so, what is the best method for doing so? For instance, should the Commission seek input from an existing or new advisory committee?

23. *National Do-Not-Call Registry.* Could the Commission utilize the existing National Do-Not-Call Registry, working in conjunction with the Federal Trade Commission (FTC), to protect PSAPs from unwanted calls? The National Do-Not-Call Registry is administered by the FTC and has been operational for almost two decades and currently protects over 240 million telephone numbers from telemarketing sales calls, or telephone solicitations. Would allowing PSAPs to register their telephone numbers on the National Do-Not-Call Registry afford them a more timely, cost-effective, and secure solution to stop many unwanted calls while shielding the identity of the relatively small number of PSAP numbers by including them among the hundreds

of millions of other telephone numbers already contained in that registry? Could this approach, in conjunction with the TCPA's existing protection from autodialed calls to "emergency telephone lines," satisfy the goals of section 6507 while providing reasonable security safeguards that preclude parties from identifying those telephone numbers associated with PSAPs and using them for malicious purposes? *See* 47 U.S.C. 227(b)(1)(A). Could the Commission work with the FTC to ensure this solution could be implemented in a timely manner?

24. Would this approach require Congress to revisit the statutory language associated with the Tax Relief Act and the TCPA to permit the Commission to implement this solution? This might include authorizing the inclusion of PSAP telephone numbers on a registry currently reserved for "residential telephone subscribers," and used by callers making telephone solicitations rather than callers making autodialed calls. *See* 47 U.S.C. 227(c). It might also include harmonizing the statutory monetary penalties associated with calling PSAP telephone numbers with those for violations of the TCPA. Alternatively, could the Commission work in conjunction with public safety organizations or their representatives to utilize any existing or planned databases of public safety numbers, rather than creating a new registry, to satisfy our obligations under the statute? If it is deemed not possible to implement section 6507 without creating significant new security risks to PSAPs, what should be done at that point?

25. *Expanded Use of the Reassigned Numbers Database.* Could the Commission expand use of the Commission's Reassigned Numbers Database (RND) as a means to prevent unwanted calls to PSAPs? The RND is designed to prevent a consumer from getting unwanted calls intended for someone who previously held their telephone number. Callers wishing to avail themselves of certain TCPA liability safe harbor provisions can query the database to determine whether a telephone number may have been reassigned since the most recent date of consent so they can avoid calling consumers who do not want to receive the calls. *See* 47 CFR 64.1200(m). To achieve its goal of avoiding robocalls to registered PSAP numbers, should the Commission expand the RND to include registered PSAP telephone numbers as well as reassigned telephone

numbers, and require autodialer operators to query the RND before placing calls? Would the inclusion of PSAP numbers, coupled with a requirement for autodialers to query the RND, effectively prevent unwanted calls to PSAPs? Would this alternative adequately protect the security of the sensitive PSAP telephone numbers while fulfilling the statutory obligation to create a PSAP Do-Not-Call registry? The Commission notes that the cost to operate the RND is recovered through usage charges collected from callers that choose to use the database. Does such a fee-based database align with Congress' intent in instructing the Commission to create the PSAP Do-Not-Call registry?

26. The Commission seeks comment on these and any other potential solutions that allow the Commission to protect registered PSAP numbers from unauthorized dissemination in a timely and cost-effective manner, while fulfilling Congress' goal of stopping unwanted calls to PSAPs, including the costs and benefits of each approach.

#### **F. Other Security Threats to PSAPs**

27. Cybersecurity events continue to affect the ability of PSAPs to respond to 911 calls, locate 911 callers, and dispatch assistance. How can the Commission aid in securing PSAPs against these types of attacks? As 911 services evolve, the ability to reach PSAPs by text, video, and data transmissions create additional vulnerabilities that may be exploited. As states and local jurisdictions have deployed text-to-911 capabilities, have PSAPs experienced attacks using text messaging as an attack vector? Have PSAPs transitioning to Next Generation 911 (NG911) systems experienced an increase in such incidents? If so, are those risks specific to NG911's technical implementation? Can the proposed Do-Not-Call registry for PSAPs mitigate risks associated with NG911 services? Can solutions used to prevent cyberattacks through the PSAP's administrative broadband connections also prevent attacks through NG911? What is needed to ensure NG911 communications with PSAPs are legitimate traffic?

28. In 2020, the Communications Security, Reliability, and Interoperability Council (CSRIC) submitted a report to the Commission regarding security risks and best practices for mitigation in

911 systems. *See Communications Security, Reliability, And Interoperability Council VII, Report on Security Risks and Best Practices for Mitigation in 9-1-1 in Legacy, Transitional, and NG 9-1-1 Implementations* (September 16, 2020). Is the report complete in its identification of security risks and best practices? What challenges, in addition to those discussed in the report, do PSAPs face in securing their operations? Are there additional best practices that PSAPs should consider adopting? What steps should the Commission take to aid in implementing best practices for PSAPs or otherwise promote cybersecurity in the PSAP environment?

29. Should the Commission consider caller ID authentication methods such as STIR/SHAKEN as a means to enhance the security of PSAP operations or promote greater trust for calls to PSAPs and those associated with 911? Providers using STIR/SHAKEN assign calls an “attestation level” that signifies what they know about the calling party and its right to use the number shown in the caller ID. Does STIR/SHAKEN sufficiently mitigate the robocall threat to PSAPs by allowing service providers to screen illegitimate 911 calls, including 911 calls to PSAPs from callers seeking to disguise their phone number or location information, more effectively? Can PSAPs use existing analytics, such as caller ID authentication, to help evaluate the trustworthiness of a call and caller? Do such analytics help PSAPs combat robocalling attacks better than a centralized database of PSAP numbers? If not, could additional STIR/SHAKEN standards, such as a unique attestation level, help distinguish between legitimate 911 calls and illegitimate calls from bad actors? Should the Commission encourage standards bodies to define such standards to be deployed by providers? Should such an attestation framework distinguish 911 calls originated by non-service initialized devices, which bypass the typical authorization conducted by originating providers, from service-initialized 911 calls? Can STIR/SHAKEN standards account for this issue and ensure that PSAPs using caller ID authentication do not negatively impact legitimate calls? Are there other technology developments or regulatory changes that would be required to facilitate the use of caller ID authentication technologies to support PSAP operations?



30. *Digital Equity and Inclusion.* The Commission, as part of its continuing effort to advance digital equity for all, including people of color, persons with disabilities, persons who live in rural or Tribal areas, and others who are or have been historically underserved, marginalized, or adversely affected by persistent poverty or inequality, invites comment on any equity-related considerations and benefits (if any) that may be associated with the proposals and issues discussed herein. *See* 47 U.S.C. 151; Executive Order No. 13985, published at 86 FR 7009, Executive Order on Advancing Racial Equity and Support for Underserved Communities Through the Federal Government (January 20, 2021). Specifically, the Commission seeks comment on how its proposals may promote or inhibit advances in diversity, equity, inclusion, and accessibility, as well as the scope of the Commission’s relevant legal authority.

## **INITIAL REGULATORY FLEXIBILITY ANALYSIS**

31. As required by the Regulatory Flexibility Act of 1980, as amended (RFA), the Commission has prepared the Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on a substantial number of small entities by the policies and rules proposed in the *FNPRM*. Written public comments are requested on the IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments on the *FNPRM* provided.

### **A. Need for, and Objectives of, the Proposed Rules**

32. Section 6507 of the Tax Relief Act required the Commission to “initiate a proceeding to create a specialized Do-Not-Call registry” for PSAPs to protect them from unwanted or illegal robocalls and to issue associated regulations after providing the public with notice and an opportunity to comment. To fulfill this mandate, in 2012 the Commission adopted rules to establish a Do-Not-Call registry for telephone numbers used by PSAPs and to prohibit the use of “automatic dialing equipment” to contact those registered numbers for non-emergency purposes.

### **B. Legal Basis**

33. The proposed rules are authorized under sections 4(i), 4(j), and 227 of the

Communications Act of 1934, as amended, 47 U.S.C. 154(i), 154(j), 227, and section 6507 of the Middle Class Tax Relief and Job Creation Act of 2012, Pub. L. 112-96, 47 U.S.C. 1473, 47 U.S.C. 6507.

### **C. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements**

34. The *FNPRM* proposes that registered PSAP telephone numbers be made available to voice service providers that will be required to block autodialed calls made to those numbers. Under this proposal, PSAPs will be permitted to register their telephone numbers on the PSAP Do-Not-Call registry. This will necessitate some administrative functions for those PSAPs, such as designating a representative to review, update, and upload their current telephone numbers to the registry. Such PSAPs will need to develop a process to verify on an annual basis that the registered numbers should continue to appear on the registry.

35. In addition, the Commission's rules already require autodialer operators seeking access to the PSAP Do-Not-Call registry to provide certain information, including all outbound telephone numbers used to place autodialed calls. The *FNPRM* proposes that autodialer operators continue to upload such numbers into the PSAP Do-Not-Call registry and update them regularly.

36. The *FNPRM* proposes that voice service providers will be provided with the registered PSAP and autodialer telephone numbers contained on the PSAP Do-Not-Call registry and will be required to block any calls that originate from a registered autodialer number when made to a registered PSAP telephone number. This will require voice service providers to develop, if they have not already done so, call blocking programs to ensure that any autodialed calls to PSAP numbers are blocked.

### **D. Steps Taken to Minimize Significant Economic Impact on Small Entities, and Significant Alternatives Considered**

37. The RFA requires an agency to describe any significant alternatives that it has considered in reaching its proposed approach, which may include the following four alternatives (among

others): (1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance or reporting requirements under the rule for small entities; (3) the use of performance, rather than design, standards; and (4) an exemption from coverage of the rule, or any part thereof, for small entities.

38. The *FNPRM* considers alternatives to requiring voice service providers to block autodialed calls and, for each alternative, the Commission requested comment on the costs and time frames required to implement the solutions discussed, including how to mitigate the impact on small businesses. Specifically, the *FNPRM* seeks comment on whether PSAPs themselves can deploy call blocking solutions and effectively block unwanted autodialed calls. It also considers whether requiring every autodialed caller to identify itself as an automated call using the Caller-ID information would allow PSAPs to block these calls more effectively.

39. In addition, the *FNPRM* considers allowing operators of autodialed calls to continue to access registered PSAP numbers. In that case, however, the Commission considers adopting more robust mechanisms or safeguards to effectively vet the identity of users who seek access to registered PSAP numbers to reduce the likelihood of providing access to those telephone numbers to bad actors that might misuse the numbers. The *FNPRM* also considers requiring callers to filter their autodialed calls through an app or software platform that would block autodialer equipment from making calls to registered PSAP numbers.

40. Further, the *FNPRM* proposes as an alternative solution the use of the existing National Do-Not-Call Registry to protect PSAPs from unwanted calls. The *FNPRM* seeks comment on whether allowing PSAPs to register their telephone numbers on the National Do-Not-Call Registry would afford them a more timely, cost-effective, and secure solution to stop many unwanted calls while shielding the identity of the relatively small number of PSAP numbers by including them among the hundreds of millions of other telephone numbers already contained in that registry. Finally, the *FNPRM* seeks comment on whether the Commission should expand

the Reassigned Numbers Database (RND) to include registered PSAP telephone numbers as well as reassigned telephone numbers, and require autodialer operators to query the RND before placing calls.

41. The Commission expects to consider the economic impact of these proposals on small entities, as identified in comments filed in response to the *FNPRM* and the IRFA, in reaching its final conclusions and taking action in this proceeding.

**E. Federal Rules that May Duplicate, Overlap, or Conflict with the Proposed Rules**

42. None.

Federal Communications Commission.

**Katura Jackson,**

*Federal Register Liaison Officer.*

[FR Doc. 2021-23698 Filed: 10/29/2021 8:45 am; Publication Date: 11/1/2021]